EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	((obfuscatation obfuscate obfuscating tamper adj resistance) and (guard check) with variable with (run adj time runtime)).clm.	US-PGPUB; USPAT	OR	ON	2007/06/02 18:21
L2	6	((obfuscatation obfuscate obfuscating tamper adj resistance) and variable with (run adj time runtime execut$3)).clm.	US-PGPUB; USPAT	OR	ON	2007/06/02 18:22
L3	0	(silent adj guard).clm.	US-PGPUB; USPAT	OR	ON	2007/06/02 18:22
S1	3	(tamperproof$3 and software).ab. and ("713"/$.ccls "380"/$.ccls. "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/05 17:03
S2	53	(tamper$7 and software).ab. and ("713"/$.ccls "380"/$.ccls. "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/19 11:55
S3	65	(tamper$7 and (software code)).ab. and ("713"/$.ccls "380"/$.ccls. "726"/$.ccls.)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/19 11:55
S4	9	("5748741").URPN.	USPAT	OR	ON	2006/06/19 11:59
S5	35	("20050210275" | "3745316" | "4172213" | "5054787" | "5123045" | "5126728" | "5159630" | "5199069" | "5365589" | "5420942" | "5548648" | "5742686" | "5745569" | "5748741" | "5768372" | "5809306" | "5812671" | "5852664" | "5915017" | "5933498" | "5933501" | "5960080" | "6041316" | "6085029" | "6240183" | "6256777" | "6263313" | "6483600" | "6507868" | "6636530" | "6668325" | "6779114" | "6782478" | "6801999" | "6901516").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/06/19 12:00
S6	1	("2005/0210275").URPN.	USPAT	OR	ON	2006/06/19 12:54
S7	3258	((713/176) or (713/187) or (713/189) or (713/194)).CCLS.	US-PGPUB; USPAT	OR	OFF	2006/06/19 12:55

EAST Search History

S8	397	S7 and (@pd > "20051222")	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/06/19 12:55
S9	1	("5748741").PN.	US-PGPUB; USPAT	OR	OFF	2006/06/20 12:13
S10	3926	((713/176) or (713/187) or (713/189) or (713/194)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/02 16:50
S11	183	S10 and (tamperproof$3 obfuscat$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/02 16:51
S12	6	("5123045" | "5509070" | "5659754" | "5666411" | "5748741" | "5768596").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/03/05 17:10
S13	6	("5123045" | "5659754" | "5748741" | "5768596" | "5892899" | "6192475").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/03/05 17:46
S14	6	("6779114").URPN.	USPAT	OR	ON	2007/03/05 17:46
S15	17	("20020026633" | "5530866" | "5659753" | "5732273" | "5974549" | "6021273" | "6023764" | "6086632" | "6128774" | "6131165" | "6151618" | "6272612" | "6279111" | "6282652" | "6629312" | "6779114" | "6851108").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/03/05 17:59
S16	4169	((713/176) or (713/187) or (713/189) or (713/194)).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/06/02 16:51
S17	197	S16 and (tamperproof$3 obfuscat$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/06/02 16:51
S18	0	("2005/0246554").URPN.	USPAT	OR	ON	2007/06/02 16:53
S19	4	("20050210275" | "4558176" | "4901231" | "5925127").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/06/02 16:58
S20	6	("5123045" | "5509070" | "5659754" | "5666411" | "5748741" | "5768596").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/06/02 18:19

Terms used **variable runtime obfuscation tamper resistance** Found **23** of **201,890**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 23 Result page: **1** 2 next

Relevance scale

1 Software and languages: Proteus: virtualization for diversified tamper-resistance

Bertrand Anckaert, Mariusz Jakubowski, Ramarathnam Venkatesan
October 2006 **Proceedings of the ACM workshop on Digital rights management DRM '06**
Publisher: ACM Press
Full text available: pdf(299.79 KB) Additional Information: full citation, abstract, references, index terms

Despite huge efforts by software providers, software protection mechanisms are still broken on a regular basis. Due to the current distribution model, an attack against one copy of the software can be reused against any copy of the software. Diversity is an important tool to overcome this problem. It allows for renewable defenses in space, by giving every user a different copy, and renewable defenses in time when combined with tailored updates. This paper studies the possibilities and limitation ...

Keywords: copyright protection, diversity, intellectual property, obfuscation, tamper-resistance, virtualization

2 Emerging applications: Obfuscation of executable code to improve resistance to static disassembly

Cullen Linn, Saumya Debray
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
Publisher: ACM Press
Full text available: pdf(155.75 KB) Additional Information: full citation, abstract, references, citings, index terms

A great deal of software is distributed in the form of executable code. The ability to reverse engineer such executables can create opportunities for theft of intellectual property via software piracy, as well as security breaches by allowing attackers to discover vulnerabilities in an application. The process of reverse engineering an executable program typically begins with disassembly, which translates machine code to assembly code. This is then followed by various decompilation steps that ai ...

Keywords: code obfuscation, disassembly

3 Software and systems: Obfuscation of design intent in object-oriented applications

Mikhail Sosonkin, Gleb Naumovich, Nasir Memon
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(368.61 KB) Additional Information: full citation, abstract, references, index terms

Protection of digital data from unauthorized access is of paramount importance. In the past several years, much research has concentrated on protecting data from the standpoint of confidentiality, integrity and availability. Software is a form of data with unique properties and its protection poses unique challenges. First, software can be reverse engineered, which may result in stolen intellectual property. Second, software can be altered with the intent of performing operations this software m ...

Keywords: code generation, refactoring, software obfuscation

4 Code optimization II: Hiding program slices for software security
Xiangyu Zhang, Rajiv Gupta
March 2003 **Proceedings of the international symposium on Code generation and optimization: feedback-directed and runtime optimization CGO '03**
Publisher: IEEE Computer Society
Full text available: pdf(1.05 MB) Additional Information: full citation, abstract, references, citings, index terms

Given the high cost of producing software, development of technology for prevention of software piracy is important for the software industry. In this paper we present a novel approach for preventing the creation of unauthorized copies of software. Our approach splits software modules into *open* and *hidden* components. The open components are installed (executed) on an unsecure machine while the hidden components are installed (executed) on a secure machine. We assume that while open ...

5 Tamper-resistant whole program partitioning
Tao Zhang, Santosh Pande, Antonio Valverde
June 2003 **ACM SIGPLAN Notices , Proceedings of the 2003 ACM SIGPLAN conference on Language, compiler, and tool for embedded systems LCTES '03**, Volume 38 Issue 7
Publisher: ACM Press
Full text available: pdf(444.16 KB) Additional Information: full citation, abstract, references, citings, index terms

Due to limited available memory (of the order of Kilobytes) on embedded devices (such as smart cards), we undertake an approach of partitioning the whole program when it does not fit in the memory. The program partitions are downloaded from the server on demand into the embedded device just before execution. We devise a method of partitioning the code and data of the program such that no information regarding the control flow behavior of the program is leaked out. This property is called tamper ...

Keywords: mobile code, program partitioning, ramper resistance, smart card

6 Software issues: Control flow based obfuscation
Jun Ge, Soma Chaudhuri, Akhilesh Tyagi
November 2005 **Proceedings of the 5th ACM workshop on Digital rights management DRM '05**
Publisher: ACM Press
Full text available: pdf(316.58 KB) Additional Information: full citation, abstract, references, index terms

A software obfuscator is a program O to transform a source program *P* for protection

against malicious reverse engineering. O should be *correct* (O(*P*) has same functionality with *P*), *resilient* (O(*P*) is resilient against attacks), and *effective* (O(*P*) is not too much slower than *P*). In this paper we describe the design of an obfuscator which consists of two parts. The first part extracts the control flow information from the program and ...

Keywords: control flow, software obfuscation

7 Session S4.2: program transformation: Leakage-proof program partitioning

Tao Zhang, Santosh Pande, Andre dos Santos, Franz Josef BrueckImayr

October 2002 **Proceedings of the 2002 international conference on Compilers, architecture, and synthesis for embedded systems CASES '02**

Publisher: ACM Press

Full text available: pdf(231.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Due to limited available memory (of the order of Kilobytes) on embedded devices (such as smart cards), we undertake an approach of partitioning a whole program. The program partitions are down-loaded from the server on demand into the embedded device just before execution. We devise a novel method of partitioning the code and data of the program such that no information regarding the control flow and behavior of the program is leaked out. In other words, by observing the program partitions that ...

Keywords: mobile code, multi-application smart card, program partitioning, tamper-resistance

8 SAFE-OPS: An approach to embedded software security

Joseph Zambreno, Alok Choudhary, Rahul Simha, Bhagi Narahari, Nasir Memon

February 2005 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 4 Issue 1

Publisher: ACM Press

Full text available: pdf(556.27 KB) Additional Information: full citation, abstract, references, index terms

The new-found ubiquity of embedded processors in consumer and industrial applications brings with it an intensified focus on security, as a strong level of trust in the system software is crucial to their widespread deployment. The growing area of *software protection* attempts to address the key steps used by hackers in attacking a software system. In this paper, we introduce a unique approach to embedded software protection that utilizes a hardware/software codesign methodology. Results d ...

Keywords: HW/SW codesign, Software protection

9 Computer security and encryption II: Some new approaches for preventing software tampering

Bin Fu, Golden Richard, Yixin Chen

March 2006 **Proceedings of the 44th annual Southeast regional conference ACM-SE 44**

Publisher: ACM Press

Full text available: pdf(124.74 KB) Additional Information: full citation, abstract, references

In this paper, we propose several methods to increase the difficulty of reverse engineering applications, with special emphasis on preventing the circumvention of copy protection mechanisms that permit only authorized users to execute the applications. We apply the hashing function to transform some constants in the software and recover them during the execution with the correct input of the password. The security of such a method depends on the hardness of the invertibility of the hashing funct ...

10 Behavioral synthesis techniques for intellectual property protection

Farinaz Koushanfar, Inki Hong, Miodrag Potkonjak

July 2005 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**, Volume 10 Issue 3

Publisher: ACM Press

Full text available: pdf(439.81 KB) Additional Information: full citation, abstract, references, index terms

We introduce dynamic watermarking techniques for protecting the value of intellectual property of CAD and compilation tools and reusable design components. The essence of the new approach is the addition of a set of design and timing constraints which encodes the author's signature. The constraints are selected in such a way that they result in a minimal hardware overhead while embedding a unique signature that is difficult to remove and forge. Techniques are applicable in conjunction with an ar ...

Keywords: Intellectual property protection, behavioral synthesis, watermarking

11 Pioneer: verifying code integrity and enforcing untampered code execution on legacy systems

Arvind Seshadri, Mark Luk, Elaine Shi, Adrian Perrig, Leendert van Doorn, Pradeep Khosla

October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available: pdf(264.30 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose a primitive, called Pioneer, as a first step towards verifiable code execution on untrusted legacy hosts. Pioneer does not require any hardware support such as secure co-processors or CPU-architecture extensions. We implement Pioneer on an Intel Pentium IV Xeon processor. Pioneer can be used as a basic building block to build security systems. We demonstrate this by building a kernel rootkit detector.

Keywords: dynamic root of trust, rootkit detection, self-check-summing code, software-based code attestation, verifiable code execution

12 Copyrights and access-rights: Experiences with the enforcement of access rights extracted from ODRL-based digital contracts

Susanne Guth, Gustaf Neumann, Mark Strembeck

October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**

Publisher: ACM Press

Full text available: pdf(241.29 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we present our experiences concerning the enforcement of access rights extracted from ODRL-based digital contracts. We introduce the generalized *Contract Schema* (CoSa) which is an approach to provide a generic representation of contract information on top of rights expression languages. We give an overview of the design and implementation of the xoRELInterpreter software component. In particular, the xoRELInterpreter interprets digital contracts that are based on rights exp ...

13 Secure and security systems: Satisfiability-based framework for enabling side-channel attacks on cryptographic software

Nachiketh R. Potlapally, Anand Raghunathan, Srivaths Ravi, Niraj K. Jha, Ruby B. Lee

March 2006 **Proceedings of the conference on Design, automation and test in Europe: Designers' forum DATE '06**
Publisher: European Design and Automation Association
Full text available: pdf(161.25 KB) Additional Information: full citation, abstract, references

Many electronic systems contain implementations of cryptographic algorithms in order to provide security. It is well known that cryptographic algorithms, irrespective of their theoretical strength, can be broken through weaknesses in their implementation. In particular, side-channel attacks, which exploit unintended information leakage from the implementation, have been established as a powerful way of attacking cryptographic systems. All side-channel attacks can be viewed as consisting of two p ...

14 Hybrid multi-core architecture for boosting single-threaded performance
Jun Yan, Wei Zhang
March 2007 **ACM SIGARCH Computer Architecture News**, Volume 35 Issue 1
Publisher: ACM Press
Full text available: pdf(410.37 KB) Additional Information: full citation, abstract, references, index terms

The scaling of technology and the diminishing return of complicated uniprocessors have driven the industry towards multicore processors. While multithreaded applications can naturally leverage the enhanced throughput of multi-core processors, a large number of important applications are single-threaded, which cannot automatically harness the potential of multi-core processors. In this paper, we propose a compiler-driven heterogeneous multicore architecture, consisting of tightly-integrated VL ...

15 Terra: a virtual machine-based platform for trusted computing
Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh
October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5
Publisher: ACM Press
Full text available: pdf(140.31 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a flexible architecture for trusted computing, called Terra, that allows applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

16 Security: Anomalous path detection with hardware support
Tao Zhang, Xiaotong Zhuang, Santosh Pande, Wenke Lee
September 2005 **Proceedings of the 2005 international conference on Compilers, architectures and synthesis for embedded systems CASES '05**
Publisher: ACM Press
Full text available: pdf(419.43 KB) Additional Information: full citation, abstract, references, index terms

Embedded systems are being deployed as a part of critical infrastructures and are vulnerable to malicious attacks due to internet accessibility. Intrusion detection systems have been proposed to protect computer systems from unauthorized penetration. Detecting an attack early on pays off since further damage is avoided and in some cases, resilient recovery could be adopted. This is especially important for embedded systems deployed in critical infrastructures such as Power Grids etc. where a tim ...

Keywords: anomalous path, anomaly detection, control flow monitoring, hardware support, monitoring granularity

17 Implementing an untrusted operating system on trusted hardware

David Lie, Chandramohan A. Thekkath, Mark Horowitz

October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5

Publisher: ACM Press

Full text available: pdf(280.87 KB) Additional Information: full citation, abstract, references, citings, index terms

Recently, there has been considerable interest in providing "trusted computing platforms" using hardware~---~TCPA and Palladium being the most publicly visible examples. In this paper we discuss our experience with building such a platform using a traditional time-sharing operating system executing on XOM~---~a processor architecture that provides copy protection and tamper-resistance functions. In XOM, only the processor is trusted; main memory and the operating system are not trusted.Our opera ...

Keywords: XOM, XOMOS, untrusted operating systems

18 Services: TinySec: a link layer security architecture for wireless sensor networks

Chris Karlof, Naveen Sastry, David Wagner

November 2004 **Proceedings of the 2nd international conference on Embedded networked sensor systems SenSys '04**

Publisher: ACM Press

Full text available: pdf(316.88 KB) Additional Information: full citation, abstract, references, citings, index terms

We introduce TinySec, the first fully-implemented link layer security architecture for wireless sensor networks. In our design, we leverage recent lessons learned from design vulnerabilities in security protocols for other wireless networks such as 802.11b and GSM. Conventional security protocols tend to be conservative in their security guarantees, typically adding 16--32 bytes of overhead. With small memories, weak processors, limited energy, and 30 byte packets, sensor networks cannot affo ...

Keywords: link layer security, sensor network security

19 Reliability and security: Java cryptography on KVM and its performance and security optimization using HW/SW co-design techniques

Yusuke Matsuoka, Patrick Schaumont, Kris Tiri, Ingrid Verbauwhede

September 2004 **Proceedings of the 2004 international conference on Compilers, architecture, and synthesis for embedded systems CASES '04**

Publisher: ACM Press

Full text available: pdf(188.08 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes a design approach to include and optimize Java based cryptographic applications into resource limited embedded devices.For easy prototyping and to be platform independent, the security applications are first developed in Java. Two Java cryptographic libraries, the Bouncy Castle API and the IAIK API are ported to a real embedded device for cost and performance evaluation. It requires 0.88Mbytes to 1.2Mbytes in the KVM footprint size and a few milliseconds to run secret key al ...

Keywords: cryptography, design, embedded systems, java, security

20 Workshop on architectural support for security and anti-virus (WASSA): Towards the issues in architectural support for protection of software execution

Weidong Shi, Hsien-Hsin S. Lee, Chenghuai Lu, Mrinmoy Ghosh
March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: pdf(436.30 KB) Additional Information: full citation, abstract, references, index terms

Recently, there is a growing interest in the research community to employ tamper-resistant processors for software protection. Many of these proposed systems rely on a specially tailored secure processor to prevent 1) illegal software duplication, 2) unauthorized software modification, and 3) unauthorized software reverse engineering. Most of these works primarily focus on the feasibility demonstration and design details rather than trying to elucidate many fundamental issues that are either "el ...

Keywords: attack, copy protection, encryption, security, tamper resistance

Results 1 - 20 of 23 Result page: **1** 2 next